REMARKS

Applicant has carefully reviewed and considered the Office Action mailed on September 10, 2003, and the references cited therewith.

Claim 1 was amended. No new claims were added. Claims 1-17 remain pending in this application.

§101 Rejection of the Claims

Claims 1-7 were rejected under 35 USC § 101 as being directed to non-statutory matter. Claim 1 has been amended to include a reference to a server where the directory is stored.

§103 Rejection of the Claims

Claims 1-17 were rejected under 35 USC § 103(a) as being unpatentable over Reid (U.S. Patent No. 6,131,120) in view of "The Microsoft Computer Dictionary, 1997", further in view of "Check Point Account Management Client, Version 1.0, 1998".

Reid describes a network security protocol in which router/gateways are used to control network traffic passing through each router/gateway.

> An enterprise directory residing on a directory server stores the names, workstations, router/gateways, servers, IP addresses locations, passwords, and encryption keys for individuals. Periodically, the directory server downloads to each router/gateway across the WAN router/gateway access lists (RALs), thereby controlling all network access across the WAN. Also periodically, the directory server downloads user control files (UCFs) to servers in the network, thereby controlling all server access across the WAN. This directory-based invention thus provides enhanced network control, and enhanced network security.

Reid, col. 6, lines 2-12. Reid, therefore, controls access to data within a network by limiting traffic through router/gateways (using a RAL at each router/gateway) and by limiting access to files within servers (using a UCF at each server). Both the RAL and the UCF are generated by a directory server and distributed periodically to their respective router/gateways and servers.

In addition, one or more of the servers can provide user authentication. Reid states that authentication at the server level is superior to that at the firewall since "distributed authentication provides greatly enhanced security over a firewall-protected network." Reid, col. 6, lines 63-65.

Applicant teaches that it can be difficult to maintain a directory for computer security at the same time that one is maintaining a directory for other purposes. As noted at p. 4, lines 16-23, maintenance of a firewall authentication database is especially burdensome in companies with a large amount of employee turnover or in companies with a large number of firewalls. Applicant teaches that it can be advantageous to configure the firewall to leverage existing databases, such as an LDAP server storing employee information such as is shown in Fig. 4.

As is described on p. 9, line 1 through p. 10, line 2 and as is shown in Fig. 3, an authorization module 206 within firewall 110 receives a request from a user to access an application or resource on the other side of firewall 110. Authorization module 206 authenticates the user, and then determines whether that user is authorized to have his access request fulfilled by querying a server 106 having an LDAP directory. The entry read from the LDAP directory that is associated with the user is compared to an authorization filter. If one or more attributes of the entry does not satisfy the filter, the user is not authorized to access the requested application or resource and the request fails. If, however, all the attributes of the entry satisfy the filter, the user is authorized to access the requested application or resource and the request is allowed through firewall 110.

Claim 1, as amended, includes a server having at least one directory and a firewall configured to intercept network resource requests from a plurality of client users. The firewall is "operative to authorize a network resource request based upon a comparison of the contents of at least part of one or more entries in said at least one directory to an authorization filter, wherein said authorization filter is generated based on a directory schema that is predefined by said entity."

The Examiner stated that since the router/gateway access list is sent to each router/gateway and controls who may have access through router/gateway,

> The examiner asserts that in order for the directory to generate the appropriate access list, each router/gateway must have transmitted its access criteria to the directory. The examiner further asserts that this criteria is an authorization filter and that in order for the directory to send back a correct access list, some comparison must have been made with directory entries and the router/gateway criteria (authorization filter).

Office Action, p. 5, third full paragraph. Applicant disagrees.

As noted above, Reid makes it clear (col. 6, lines 2-12) that all security information is stored within an enterprise directory and that periodically that directory downloads RALs and UCFs to router/gateways and servers, respectively. "Because the directory knows the location and IP address of each user, and the location and IP address of each router/gateway, a directory application can periodically populate the RAL in each router/gateway on the network using LDAP. Entries in the directory thereby control the entire network and the network router/gateway configuration management is automated." Col. 6, lines 19-25. Therefore, despite the Examiner's statement that "in order for the directory to send back a correct access list, some comparison must have been made with directory entries and the router/gateway criteria (authorization filter)," no such authorization filter is provided in Reid. At least one limitation of claims 1-7 is, therefore, not present in any of the references cited by the Examiner. Reconsideration of claims 1-7 is respectfully requested.

Claim 8 is to an authentication method which determines if a user is authorized to access an application or a resource by applying an authorization filter to an entry associated with the user stored in a directory. Once again, Reid does not describe the application of an authorization filter to an entry read from a directory. At least one limitation of claims 8-16 is, therefore, not present in any of the references cited by the Examiner. Reconsideration of claims 8-16 is respectfully requested.

Claim 17 is a computer program product which includes program code for applying an authorization filter to an entry associated with the user stored in a directory. Once again, Reid does not describe the application of an authorization filter to an entry read from a directory. At least one limitation of claim 17 is, therefore, not present in any of the references cited by the Examiner. Reconsideration of claim 17 is respectfully requested.

Claims 6 and 13 were rejected under 35 USC § 103(a) as being unpatentable over Reid as applied to 1 and 8 above, and further in view of Elgamal (U.S. Patent No. 5,657,390).

Neither Reid nor Elgamel teach the use of an authorization filter as described by Applicant. In addition, Elgamal does not describe the use of a secure socket layer communication to distribute an entry in an LDAP database as taught by Applicant and claimed in claims 6 and 13. Reconsideration of claims 6 and 13 is respectfully requested.

Claims 3 and 10 were rejected under 35 USC § 103(a) as being unpatentable over Reid as applied to claims 1 and 8 above, and further in view of Wesinger (U.S. Patent No. 5,898,830).

Neither Reid nor Wesinger teach the use of an authorization filter as described by Applicant. In addition, Wesinger does not describe the use of GUI to specify how to implement the authorization filer as taught by Applicant and claimed in claims 3 and 10. Reconsideration of claims 3 and 10 is respectfully requested.

Claims 11 and 12 were rejected under 35 USC § 103(a) as being unpatentable over Reid in view of Wesinger as applied to claims 3 and 10 above, and further in view of Reid as applied to claims 4 and 5 above.

Neither Reid nor Wesinger teach the use of an authorization filter as described by Applicant. In addition, Wesinger does not describe the methods used to implement the authorization filer as taught by Applicant and claimed in claims 11 and 12. Reconsideration of claims 11 and 12 is respectfully requested.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743

Respectfully submitted,

Thomas D. Ashoff, et al.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6909

Date January 12, 2004 By Thomas F. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 12 day of January, 2004.

GINA JOHNS
Name

Gina Johns
Signature